IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	§	
Joseph Won John	§	Group Art Unit: 2157
	§	
Serial No.: 10/809,586	§	Examiner: Shiu, Ho T.
	§	
Filed: 03/25/2004	§	Atty Docket No.: AUS920040008US1
	§	
Title: Establishing Trust In An Email	§	Customer No.: 34533
Client	§	
	§	Confirmation No. 7114

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF

Honorable Commissioner:

This is an Appeal Brief filed pursuant to 37 CFR § 41.37 in response to the Final Office
Action of June 12, 2008 (hereinafter the "Final Office Action"), and pursuant to the
Notice of Appeal filed September 3, 2008.

REAL PARTY IN INTEREST

The real party in interest in accordance with 37 CFR § 41.37(c)(1)(i) is the patent
assignee, International Business Machines Corporation ("IBM"), a New York corporation
having a place of business at Armonk, New York 10504.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences within the meaning of 37 CFR §
41.37(c)(1)(ii).

STATUS OF CLAIMS

Status of claims in accordance with 37 CFR § 41.37(c)(1)(iii): Twenty-four (24) claims were filed in the original application in this case. Claims 2, 10, and 18 were cancelled in a Response filed on March 18, 2008. Claims 1, 3-9, 11-17, and 19-24 remain in the present application and are rejected in the final Office Action. Claims 1, 3-9, 11-17, and 19-24 are on appeal.

STATUS OF AMENDMENTS

Status of amendments in accordance with 37 CFR § 41.37(c)(1)(iv): No amendments were submitted after final rejection. The claims as currently presented are included in the Appendix of Claims that accompanies this Appeal Brief.

SUMMARY OF CLAIMED SUBJECT MATTER

Appellants provide the following concise summary of the claimed subject matter according to 37 CFR § 41.37(c)(1)(v). This summary includes a concise explanation of the subject matter defined in each of the independent claims involved in the appeal. This summary includes references to the specification by page and line number and to the drawings by reference characters. The independent claims involved in this appeal are claims 1, 9, and 17.

Claim 1 recites a method for establishing trust in an email client (page 5, lines 24-26, and Figure 1). Claim 1 includes accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address (page 16, lines 26-28, and Figure 3, elements 302, 304, and 306). Claim 1 also includes determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address (page 17, lines 12-14, and Figure 3, elements 302, 310, and 312). Claim 1 includes, if the email client is not trusted according to the email client's network address, receiving authentication data from the email client and determining whether the email client is trusted according to the authentication data (page 17, lines 24-27, and Figure 3, elements 314, 316, and 320).

Claim 1 also includes, if the email client is not trusted according to the email client's network address and the email client is not trusted according to the authentication data, receiving a sender domain name for an email message from the email client and determining whether the email client is trusted according to the sender domain name (page 18, lines 11-15, and Figure 3, elements 322, 324, and 326), wherein determining whether the email client is trusted according to the sender domain name further comprises requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain (page 19, lines 7-12, and Figure 4, elements 107 and 402).

Claim 9 recites a system for establishing trust in an email client (page 4, line 28 – page 5, line 7, page 5, lines 24-26, and Figure 1). The system of claim 9 includes means for accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address (page 4, line 28 – page 5, line 7, page 16, lines 26-28, and Figure 3, elements 302, 304, and 306). The system of claim 9 also includes means for determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address (page 4, line 28 – page 5, line 7, page 17, lines 12-14, and Figure 3, elements 302, 310, and 312). The system of claim 9 also includes means for receiving authentication data from the email client and means for determining whether the email client is trusted according to the authentication data if the email client is not trusted according to the email client's network address (page 4, line 28 – page 5, line 7, page 17, lines 24-27, and Figure 3, elements 314, 316, and 320). The system of claim 9 also includes means for receiving a sender domain name for an email message from the email client and means for determining whether the email client is trusted according to the sender domain name if the email client is not trusted according to the email client's network address and the email client is not trusted according to the authentication data (page 4, line 28 – page 5, line 7, page 18, lines 11-15, and Figure 3, elements 322, 324, and 326), wherein means for determining whether the email client is trusted according to the sender domain name further comprises means for requesting from a domain name

service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain (page 4, line 28 – page 5, line 7, page 19, lines 7-12, and Figure 4, elements 107 and 402).

Claim 17 recites a computer program product for establishing trust in an email client (page 5, line 9-20, page 5, lines 24-26, and Figure 1). Claim 17 includes a recording medium (page 5, line 9-20) and means, recorded on the recording medium, for accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address (page 5, line 9-20, page 16, lines 26-28, and Figure 3, elements 302, 304, and 306). Claim 17 also includes means, recorded on the recording medium, for determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address (page 5, line 9-20, page 17, lines 12-14, and Figure 3, elements 302, 310, and 312). Claim 17 also includes means, recorded on the recording medium, for receiving authentication data from the email client and means, recorded on the recording medium, for determining whether the email client is trusted according to the authentication data if the email client is not trusted according to the email client's network address (page 5, line 9-20, page 17, lines 24-27, and Figure 3, elements 314, 316, and 320). Claim 17 also includes means, recorded on the recording medium, for receiving a sender domain name for an email message from the email client and means, recorded on the recording medium, for determining whether the email client is trusted according to the sender domain name if the email client is not trusted according to the email client's network address and the email client is not trusted according to the authentication data (page 5, line 9-20, page 18, lines 11-15, and Figure 3, elements 322, 324, and 326), wherein means, recorded on the recording medium, for determining whether the email client is trusted according to the sender domain name further comprises means, recorded on the recording medium, for requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain (page 5, line 9-20, page 19, lines 7-12, and Figure 4, elements 107 and 402).

GROUNDS OF REJECTION

In accordance with 37 CFR § 41.37(c)(1)(vi), Appellants provide the following concise statement for each ground of rejection:

1. Claims 1, 4-9, 12-17, and 20-24 stand rejected under 35 U.S.C. § 102 as being anticipated by Weatherby, et al. (U.S. Publication No. 2004/0054741).

2. Claims 3, 11, and 19 stand rejected for obviousness under 35 U.S.C. §103 as being unpatentable over Weatherby, et al. (U.S. Publication No. 2004/0054741) in view of Lalonde, et al. (U.S. Publication No. 2004/0068542).

ARGUMENT

Appellants present the following argument pursuant to 37 CFR § 41.37(c)(1)(vii) regarding the grounds of rejection on appeal in the present case.

**Argument Regarding The First Ground Of Rejection
On Appeal: 1, 4-9, 12-17, And 20-24 Stand Rejected
Under 35 U.S.C. § 102 As Being Anticipated By
Weatherby, Et Al. (U.S. Publication No. 2004/0054741)**

Claims 1, 4-9, 12-17, and 20-24 stand rejected under 35 U.S.C. § 102 as being anticipated by Weatherby, *et al.* (U.S. Publication No. 2004/0054741) (hereafter, 'Weatherby'). "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Independent claim 1 of the present application recites:

1.   A method for establishing trust in an email client, the method comprising:

accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address;

determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address;

if the email client is not trusted according to the email client's network address, receiving authentication data from the email client and determining whether the email client is trusted according to the authentication data; and

if the email client is not trusted according to the email client's
network address and the email client is not trusted according to the
authentication data, receiving a sender domain name for an email
message from the email client and determining whether the email
client is trusted according to the sender domain name, wherein
determining whether the email client is trusted according to the
sender domain name further comprises requesting from a domain
name service a resource record of a type that lists for a sender
domain network addresses of email exchanges that are authorized
to act as outbound email exchanges for the sender domain.

As explained in more detail below, Weatherby does not disclose and enable each and
every element of claim 1. As such, Weatherby cannot be said to anticipate the claims of
the present application within the meaning of 35 U.S.C. § 102.

**Weatherby Does Not Disclose Requesting From A Domain Name
Service A Resource Record Of A Type That Lists For A Sender
Domain Network Addresses Of Email Exchanges That Are Authorized
To Act As Outbound Email Exchanges For The Sender Domain**

The Office Action takes the position that Weatherby at paragraph 0029 - paragraph 0030,
lines 1-7, paragraph 0033, lines 1-6, and paragraph 0041, lines 1-18 discloses the
following portion of claim 1: wherein determining whether the email client is trusted
according to the sender domain name further comprises requesting from a domain name
service a resource record of a type that lists for a sender domain network addresses of
email exchanges that are authorized to act as outbound email exchanges for the sender
domain. Applicants respectfully note in response, however, that what Weatherby at
paragraph 0029 – paragraph 0030, lines 1-7 actually discloses is:

[0029] In the preferred embodiment illustrated in FIG. 1, the logic begins
when a sender transmits an E-mail message which is to a recipient on a
system equipped with the present invention (Block 100). Typically, with
such messages, the sender's E-mail address is entered into the From field
of the SMTP header associated with the E-mail message. While the
description of a preferred embodiment of the present invention focuses on

the content of the From field, it should be apparent to those skilled in the art that alternative header field content could be used, including, but not limited to, the x-ReplyTo field, the sender's name, the sender's Internet Protocol ("IP") address, or the like, without departing from the spirit or the scope of the present invention.

[0030] When an incoming message is received by a preferred embodiment of the present invention, the sender's E-mail address is preferably compared against a system-wide list of E-mail addresses which are to be blocked (Block 105). Such a list may include individual E-mail addresses, such as tom@blah.com, or E-mail addresses from entire domains, such as *@blah.com.

In addition, what Weatherby at paragraph 0033, lines 1-6, actually discloses is:

[0033] If an incoming message has not been blocked by comparison to the system-wide block list or the sender's block list, the sender's E-mail address is compared against the recipient's verified list (Block 130). If the E-mail address appears in the recipient's verified list, the message is delivered to the recipient's inbox (Block 135).

Furthermore, what Weatherby at paragraph 0041, lines 1-18, actually discloses is:

[0041] While it is true that a UCE distributor could potentially produce a robot that will automatically click on any links returned within an email, to do so, the UCE distributor must use one or more non-spoofed email accounts, must receive all challenge handshake messages, and must engage in a three-way process that corroborates illegal actions. While it is difficult to stop someone intent on fooling any system, the present invention can also employ additional techniques to thwart robots. Furthermore, the verification techniques employed by the present invention require UCE distributors to give up their anonymity because the sender's IP address, domain name, and HTTP IP address are all preferably logged and reported when the sender validates with the present invention. An additional benefit of the present invention is its ability to automatically add all sender E-mail addresses whose challenge message bounces due to unknown user or other SMTP errors to the recipients' blocked list.

That is, Weatherby at paragraph 0029 – paragraph 0030, lines 1-7, paragraph 0033, lines 1-6, and paragraph 0041, lines 1-18, discloses comparing the sender's E-mail address against a system-wide list of E-mail addresses which are to be blocked. Weatherby's

comparison of the sender's E-mail address against a system-wide list of E-mail addresses which are to be blocked does not disclose requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain as claimed in the present application. Weatherby's system-wide list of E-mail addresses which are to be blocked is not a resource record, as claimed in the present application. A resource record, as claimed in the present application, is requested from a domain name service, and lists for a sender domain network, addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain. In contrast, Weatherby's system-wide list of E-mail addresses is located on the email client's system – not requested from a domain name service, and lists blocked email addresses – not addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain. In fact, at no point in the reference does Weatherby even mention "a resource record", "domain name service", or an "email exchange." Without disclosing requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain, as claimed in the present application, Weatherby does not disclose each and every element and limitation of claim 1. Because Weatherby does not disclose each and every element and limitation of claim 1 of the present application, Weatherby does not anticipate claim 1 of the present application and the rejections under 35 U.S.C. § 102 should therefore be withdrawn.

Weatherby Does Not Enable Each And Every Element Of The Claims Of The Present Application

Not only must Weatherby disclose each and every element of the claims of the present application within the meaning of *Verdegaal* in order to anticipate Applicants' claims, but also Weatherby must be an enabling disclosure of each and every element of the claims of the present application within the meaning of *In re Hoeksema*. In *Hoeksema*, the claims were rejected because an earlier patent disclosed a structural similarity to the Applicant's chemical compound. The court in Hoeksema stated: "We think it is sound law, consistent with the public policy underlying our patent law, that before any

9

publication can amount to a statutory bar to the grant of a patent, its disclosure must be such that a skilled artisan could take its teachings in combination with his own knowledge of the particular art and be in possession of the invention." *In re Hoeksema,* 399 F.2d 269, 273, 158 USPQ 596, 600 (CCPA 1968). The meaning of *Hoeksema* for the present case is that unless Weatherby places Applicants' claims in the possession of a person of ordinary skill in the art, Weatherby is legally insufficient to anticipate Applicants' claims under 35 U.S.C. § 102(b). As explained above, Weatherby does not disclose each and every element and limitation of independent claim 1 of the present application. Because Weatherby does not disclose each and every element and limitation of the independent claims, Weatherby cannot possibly place the elements and limitations of independent claim 1 in the possession of a person of ordinary skill in the art. Weatherby cannot, therefore, anticipate claim 1 of the present application.

Relations Among Claims

Independent claims 9 and 17 are system and computer program product claims, respectively, for establishing trust in an email client corresponding to independent method claim 1. Claim 1 is allowable for the reasons set forth above. Claims 9 and 17 are allowable for the same reasons that claim 1 is allowable. The rejections of claims 9 and 17 therefore should be withdrawn, and claims 9 and 17 should be allowed.

Claims 4-8, 12-16, and 20-24 depend respectively from independent claims 1, 9, and 17. Each dependent claim includes all of the limitations of the independent claim from which it depends. Because Weatherby does not disclose or enable each and every element of the independent claims, Weatherby does not disclose or enable each and every element of the dependent claims of the present application. As such, the rejections of claims 4-8, 12-16, and 20-24 should also be withdrawn and the claims should be allowed.

Argument Regarding The Second Ground Of Rejection
On Appeal: 3, 11, And 19 Stand Rejected For Obviousness
Under 35 U.S.C. §103 As Being Unpatentable Over
Weatherby, Et Al. (U.S. Publication No. 2004/0054741) In
View Of Lalonde, Et Al. (U.S. Publication No. 2004/0068542)

Claims 3, 11, and 19 stand rejected for obviousness under 35 U.S.C. § 103(a) as being

unpatentable over Weatherby, in view of Lalonde (U.S. Publication No. 2004/0068542

A1). The question of whether Applicants claims are obvious or not is examined in light

of: (1) the scope and content of the prior art; (2) the differences between the claimed

invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant

secondary considerations, including commercial success, long felt but unsolved needs,

and failure of other. *KSR Int'l Co. v. Teleflex Inc.*, No. 04-1350, slip op. at 2 (U.S. April

30, 2007). Although Applicants recognize that such an inquiry is an expansive and

flexible one, the Office Action must nevertheless demonstrate a prima facie case of

obviousness to reject Applicants claims for obviousness under 35 U.S.C. § 103(a). *In re*

Khan, 441 F.3d 977, 985-86 (Fed. Cir. 2006). To establish a prima facie case of

obviousness, the proposed combination of Weatherby and Lalonde must teach or suggest

each and every element and limitation of dependent claims 3, 11, and 19. *In re Royka*,

490 F.2d 981, 985, 180 USPQ 580, 583 (CCPA 1974). Dependent claims 3, 11, and 19

depend from independent claims 1, 9, and 17 and include all the limitations of the

independent claims from which they depend. In rejecting dependent claims 3, 11, and 19,

the Office Action relies on Weatherby as disclosing each and every element of

independent claims 1, 9, and 17. As shown above, Weatherby does not disclose each and

every element and limitation of claims 1, 9, and 17. The proposed combination of

Weatherby and Lalonde therefore cannot possibly teach or suggest each and every

element of dependent claims 3, 11, and 19. As such, the proposed combination of

Weatherby and Lalonde cannot be used to establish a prima facie case of obviousness and

the rejections should be withdrawn.

The Office Action Does Not Examine
Applicants' Claims Pursuant To *Graham*

In addition to the fact that the Office Action has not established a prima facie of obviousness, there is another reason that the rejection of claims 3, 11, and 19 should be withdrawn: The Office Action does not examine Applicants' claims in light of the factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). The question of whether Applicants' claims are obvious or not is examined in light of: (1) the scope and content of the prior art; (2) the differences between the claimed invention and the prior art; (3) the level of ordinary skill in the art; and (4) any relevant secondary considerations, including commercial success, long felt but unsolved needs, and failure of others. *KSR Int'l Co. v. Teleflex Inc.*, No. 04-1350, slip op. at 2 (U.S. April 30, 2007); *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966). "To facilitate review, this analysis should be made explicit." *KSR*, slip op. at 14 (citing *In re Kahn*, 441 F. 3d 977, 988 (Fed. Cir. 2006)). That is, the Office Action must make explicit an analysis of the factual inquiries set forth in *Graham*. In present case, however, the Office Action does not even mention the factual inquiries set forth in *Graham*. As such, the rejections of claims 3, 11, and 19 under 35 U.S.C. § 103 are improper and should be withdrawn.
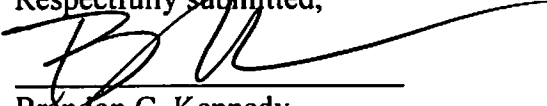
Conclusion Of Appellant's Arguments

Claims 1, 4-9, 12-17, and 20-24 stand rejected under 35 U.S.C. § 102 as being anticipated by Weatherby. For the reasons set forth above, Weatherby does not disclose or enable each and every element of Applicants' claims. Claims 1, 4-9, 12-17, and 20-24 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 1, 4-9, 12-17, and 20-24.

Claims 3, 11, and 19 stand rejected for obviousness under 35 U.S.C. § 103 as being unpatentable over Weatherby in view of Lalonde. For the reasons set forth above, however, the proposed combination of Weatherby and Lalonde cannot be used to establish a prima facie case of obviousness against the claims of the present application. The rejection of claims 3, 11, and 19 should therefore be withdrawn and the claims

should be allowed. Applicants respectfully request reconsideration of claims 3, 11, and 19.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 09-0465 for any fees required or overpaid.

Respectfully submitted,

Date: <u>November 3, 2008</u>   By: _____

Brandon C. Kennedy
Reg. No. 61,471
Biggers & Ohanian, LLP
P.O. Box 1469
Austin, Texas 78767-1469
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPELLANTS

**APPENDIX OF CLAIMS
ON APPEAL IN PATENT APPLICATION OF
JOSEPH WON JOHN, SERIAL NO. 10/809,586**

<u>CLAIMS</u>

Listing of Claims:

1.   A method for establishing trust in an email client, the method comprising:

accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address;

determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address;

if the email client is not trusted according to the email client's network address, receiving authentication data from the email client and determining whether the email client is trusted according to the authentication data; and

if the email client is not trusted according to the email client's network address and the email client is not trusted according to the authentication data, receiving a sender domain name for an email message from the email client and determining whether the email client is trusted according to the sender domain name, wherein determining whether the email client is trusted according to the sender domain name further comprises requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain.

2.   (Cancelled)

3.   The method of claim 1 wherein determining whether the email client is trusted according to the sender domain name further comprises determining whether a domain name service resource record associates the email client's network

address with the sender domain name, the DNS resource record being of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain.

4. The method of claim 1 wherein the email client is trusted according to the authentication data, and the method further comprises storing the email client's network address in association with a trust time limit in the list of trusted network addresses.

5. The method of claim 1 further comprising:

accepting in the email server a connection from an email client requesting delivery of an email message according to a protocol that includes client authentication, wherein the connection includes the network address of the email client requesting delivery of an email message;

authenticating the email client requesting delivery of an email message;

delivering the email message to the email client requesting delivery of an email message; and

storing the network address of the email client requesting delivery of an email message in association with a trust time limit in the list of trusted network addresses.

6. The method of claim 1 wherein the email client is an email exchange that accepts outbound email messages only from trusted senders.

7. The method of claim 1 wherein receiving a sender domain name further comprises receiving the sender domain name in an SMTP MAILFROM message.

8. The method of claim 1 wherein the email client is not trusted according to the email client's network address, the email client is not trusted according to the authentication, the email client is not trusted according to the sender domain name, and the method further comprises sending an error message to the email client and closing the connection.

9. A system for establishing trust in an email client, the system comprising:

means for accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address;

means for determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address;

means for receiving authentication data from the email client and means for determining whether the email client is trusted according to the authentication data if the email client is not trusted according to the email client's network address; and

means for receiving a sender domain name for an email message from the email client and means for determining whether the email client is trusted according to the sender domain name if the email client is not trusted according to the email client's network address and the email client is not trusted according to the authentication data, wherein means for determining whether the email client is trusted according to the sender domain name further comprises means for requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain.

10. (Cancelled)

11. The system of claim 9 wherein means for determining whether the email client is trusted according to the sender domain name further comprises means for determining whether a domain name service resource record associates the email client's network address with the sender domain name, the DNS resource record being of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain.

12. The system of claim 9 wherein the email client is trusted according to the authentication data, and the system further comprises means for storing the email client's network address in association with a trust time limit in the list of trusted network addresses.

13. The system of claim 9 further comprising:

means for accepting in the email server a connection from an email client requesting delivery of an email message according to a protocol that includes client authentication, wherein the connection includes the network address of the email client requesting delivery of an email message;

means for authenticating the email client requesting delivery of an email message;

means for delivering the email message to the email client requesting delivery of an email message; and

means for storing the network address of the email client requesting delivery of an email message in association with a trust time limit in the list of trusted network addresses.

14. The system of claim 9 wherein the email client is an email exchange that accepts outbound email messages only from trusted senders.

15. The system of claim 9 wherein means for receiving a sender domain name further comprises means for receiving the sender domain name in an SMTP MAILFROM message.

16. The system of claim 9 further comprising means for sending an error message to the email client and means for closing the connection if the email client is not trusted according to the email client's network address, the email client is not trusted according to the authentication, and the email client is not trusted according to the sender domain name.

17. A computer program product for establishing trust in an email client, the computer program product comprising:

a recording medium;

means, recorded on the recording medium, for accepting in an email server a data communications connection from an email client, wherein the connection includes the email client's network address;

means, recorded on the recording medium, for determining from a stored list of trusted network addresses whether the email client is trusted according to the email client's network address;

means, recorded on the recording medium, for receiving authentication data from the email client and means, recorded on the recording medium, for determining whether the email client is trusted according to the authentication data if the email client is not trusted according to the email client's network address; and

means, recorded on the recording medium, for receiving a sender domain name for an email message from the email client and means, recorded on the recording

18

medium, for determining whether the email client is trusted according to the sender domain name if the email client is not trusted according to the email client's network address and the email client is not trusted according to the authentication data, wherein means, recorded on the recording medium, for determining whether the email client is trusted according to the sender domain name further comprises means, recorded on the recording medium, for requesting from a domain name service a resource record of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain.

18. (Cancelled)

19. The computer program product of claim 17 wherein means, recorded on the recording medium, for determining whether the email client is trusted according to the sender domain name further comprises means, recorded on the recording medium, for determining whether a domain name service resource record associates the email client's network address with the sender domain name, the DNS resource record being of a type that lists for a sender domain network addresses of email exchanges that are authorized to act as outbound email exchanges for the sender domain.

20. The computer program product of claim 17 wherein the email client is trusted according to the authentication data, and the computer program product further comprises means, recorded on the recording medium, for storing the email client's network address in association with a trust time limit in the list of trusted network addresses.

21. The computer program product of claim 17 further comprising:

means, recorded on the recording medium, for accepting in the email server a connection from an email client requesting delivery of an email message

according to a protocol that includes client authentication, wherein the connection includes the network address of the email client requesting delivery of an email message;

means, recorded on the recording medium, for authenticating the email client requesting delivery of an email message;

means, recorded on the recording medium, for delivering the email message to the email client requesting delivery of an email message; and

means, recorded on the recording medium, for storing the network address of the email client requesting delivery of an email message in association with a trust time limit in the list of trusted network addresses.

22. The computer program product of claim 17 wherein the email client is an email exchange that accepts outbound email messages only from trusted senders.

23. The computer program product of claim 17 wherein means, recorded on the recording medium, for receiving a sender domain name further comprises means, recorded on the recording medium, for receiving the sender domain name in an SMTP MAILFROM message.

24. The computer program product of claim 17 further comprising means, recorded on the recording medium, for sending an error message to the email client and means, recorded on the recording medium, for closing the connection if the email client is not trusted according to the email client's network address, the email client is not trusted according to the authentication, and the email client is not trusted according to the sender domain name.

**APPENDIX OF EVIDENCE
ON APPEAL IN PATENT APPLICATION OF
JOSEPH WON JOHN, SERIAL NO. 10/809,586**

This is an evidence appendix in accordance with 37 CFR § 41.37(c)(1)(ix).

There is in this case no evidence submitted pursuant to 37 CFR §§ 1.130, 1.131, or 1.132, nor is there in this case any other evidence entered by the examiner and relied upon by the Appellants.

RELATED PROCEEDINGS APPENDIX

This is a related proceedings appendix in accordance with 37 CFR § 41.37(c)(1)(x).

There are no decisions rendered by a court or the Board in any proceeding identified pursuant to 37 CFR § 41.37(c)(1)(ii).